AFFIDAVIT

I, Matthew J. Riportella, do under oath depose a state:

I. INTRODUCTION

Agent Background

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI since June 2012. I am currently assigned to the FBI Boston Division's Providence Rhode Island Complex Financial Crimes Task Force ("PRICFCTF"), which is comprised of law enforcement officers from the FBI, Rhode Island State Police ("RISP"), United States Secret Service ("USSS") and other federal law enforcement agencies. As a member of the PRICFCTF, I am responsible for investigating white collar crimes in Rhode Island. Previously, I was assigned to the FBI Boston Divisions' Organized Crime Task Force. I have experience investigating illegal gambling, narcotics, extortion, money laundering, kidnapping, wire fraud, mail fraud and other federal crimes. My investigations have included the use of surveillance techniques, and the execution of search, seizure, and arrest warrants.

Purpose

2. I make this affidavit in support of an application for an arrest warrant and criminal complaint charging Luckson LOUISSAINT (LOUISSAINT), DOB [redacted], Social Security Number: [redacted] with Conspiracy to Commit Mail, Wire, and Bank Fraud (18 U.S.C. § 1349), Access Device Fraud (18 U.S.C. § 1029(a)(5)), and Aggravated Identity Theft (18 U.S.C. § 1028A) ("Specified Federal Offenses"). LOUISSAINT resides at [redacted] Coyle Ave [redacted] Pawtucket, RI and is described as a Black male, 31 years old, 5'7, weighing approximately 160 pounds with dark hair (hereinafter referred to as the "SUBJECT PERSON").

3. I also make this affidavit in support of Applications for a Search Warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a search of:

a. the SUBJECT PERSON, Luckson LOUISSAINT, as more particularly described in Attachment A-1 (attached hereto and incorporated herein by reference) at whatever location

he may be found, for the items described in Attachment B-1; and

b. [redacted] Coyle Ave [redacted] Pawtucket, RI (the SUBJECT PREMISES), as more particularly described in Attachment A-2 (attached and incorporated herein by reference) for the items described in Attachment B-2,

4. As set forth below, there is probable cause to believe that located on the SUBJECT PERSON and in the SUBJECT PREMISES is evidence, fruits, and instrumentalities of violations the Specified Federal Offenses.

5. The facts set forth in the Affidavit are based on my personal observations, my training and experience, information obtained from other agents, witnesses, and records obtained during the course of the investigation. Because I submit this Affidavit for the limited purpose of showing probable cause, I have not included in this Affidavit each and every fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue an arrest warrant for the individuals identified herein and to search the email accounts set forth herein. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. PROBABLE CAUSE

6. As described herein, from at least March 2020 through October 2020, LUCKSON LOUISSAINT has conspired with James Legerme, Tony Mertile, and others, to provide information and receive fraudulently issued debit cards, all in furtherance of the receipt of fraudulent UI benefits.

A. Post- CARES Act Unemployment Fraud Schemes in Rhode Island and Nationwide.

7. Since early April 2020, the FBI, RISP, Internal Revenue Service-Criminal Investigations ("IRS-CI"), Department of Labor- Office of Inspector General ("Labor-OIG"), United States Postal Inspection Service ("USPIS") and the United States Secret

Service ("USSS"), with the assistance of other federal agencies, have been investigating a large volume of fraudulent UI claims submitted to the Rhode Island Department of Labor & Training ("RIDLT") and other state UI benefit agencies. These claims were submitted online using an individual's personally identifiable information ("PII") to include their name, DOB and SSN. These claims were paid out by the State of Rhode Island and other state UI agencies via electronic bank or wire transfers to bank accounts and/or to debit cards, identified by the applicant when the application for UI benefits was submitted.

UNEMPLOYMENT INSURANCE

8. Benefits that were available in 2020 and 2021 through state unemployment insurance agencies, such as RIDLT, included the traditional unemployment insurance benefits, as well as benefits that became available as federal legislation was passed at the outset and during the pendency of the COVID-19 pandemic. Because the conduct described herein involves various types of UI benefits sought from and paid by multiple state UI agencies, I have summarized some of these benefit programs.

9. The Unemployment Insurance Program ("UI Program") is a joint federal-state partnership administered on behalf of the U.S. Department of Labor by state workforce agencies ("SWA"), also commonly referred to as UI agencies, in each state. In Rhode Island, the UI Program is operated by the RIDLT, the RI UI agency / SWA. The UI Program is designed to provide benefits to persons who are out of work through no fault of their own. UI benefits are generally funded through state employment taxes paid by employers. In order to qualify for traditional UI benefits, the applicant must have earned wages which were taxed, for a qualifying period of time. Self-employed individuals, independent contractors and non-traditional workers whose income is outside of a traditional employment relationship (sometimes referred to as gig employees) not paying employment taxes, are generally not covered by UI programs.

10. On March 27, 2020, the CARES Act provided additional assistance to workers who would otherwise not qualify for traditional UI benefits. The CARES Act provided assistance in the form of Pandemic Unemployment Assistance ("PUA"),

Pandemic Emergency Unemployment Compensation ("PEUC") and Federal Pandemic Unemployment Compensation ("FPUC").

11. PUA generally provides benefits to certain individuals who would not qualify for traditional UI programs, and are unemployed, partially unemployed, or unable to work due to COVID-19 related reasons. Individuals who are able to telework with pay are not eligible for PUA assistance. PUA initially provided up to 39 weeks of benefits to qualifying individuals which were set to expire on December 31, 2020. On or about December 27, 2020, the Continued Assistance for Unemployed Workers of 2020 Act was signed into law. This Act extended the payment of PUA benefits for up to 50 weeks through March 14, 2021. Then on March 11, 2021, the American Rescue Plan Act of 2021 ("ARPA") was signed into law. Under ARPA, PUA benefits for up to 79 weeks have been extended through September 6, 2021. The PUA program is administered by the SWA / UI agency in each state, but the benefits are 100% funded by the federal government. A PUA claim is a claim for benefits against income earned or expected to be earned by the claimant in a particular state. The claimant must certify to the particular SWA / UI agency administering the benefits that the claimant is able to go to work each day, and, if offered a job, the claimant must be able to accept it. The claimant must certify this information on a weekly basis during the benefits period. The claimant is also responsible for reporting any income earned on a weekly basis to the SWA / UI agency to which they submitted a claim.

12. PEUC was established to extend the term for UI benefits and provided up to an additional 13 weeks of UI benefits to individuals who have exhausted their regular UI benefits under state or federal law and have no rights to UI under any other federal state or law. Under the Continued Assistance for Unemployed Workers of 2020 Act, PEUC benefits were extended to provide an additional 11 weeks of benefits for a maximum of 24 weeks through March 14, 2021. Under ARPA, PEUC benefits have been extended for up to 53 weeks through September 6, 2021.

13. Separately, FPUC provided an additional $600 per week in benefits through July 2020, to individuals who were collecting UI, PUA and PEUC benefits.

FPUC benefits are 100% funded by the federal government. From August 1, 2020 through September 5, 2020, PUA and UI claimants were eligible to receive Federal Lost Wage Assistance ("FLWA") in the amount of $300 per week funded by the Federal Emergency Management Agency ("FEMA"). Under the Continued Assistance for Unemployed Workers of 2020 Act, an additional $300 in weekly FPUC benefits was extended from December 26, 2020 through March 14, 2021. Then under ARPA, FPUC benefits of $300 have been extended through September 6, 2021.

LOUISSAINT is Identified as a Co-Conspirator

14. In our investigation, Tony Mertile, Junior Mertile, James Legerme, and Allen Bien-Aime, all residents of Florida, were identified as persons who were conspiring to use bank accounts to receive payments for fraudulent UI claims submitted to the RIDLT and to other state SWAs/UI systems and for fraudulent tax refunds; fraudulently access the bank accounts opened using PII of other persons and into which those fraudulently obtained funds were deposited; and withdraw fraudulently obtained UI benefits and tax refunds from the fraudulently opened bank accounts.

15. On October 6, 2020, Tony Mertile, Junior Mertile, James Legerme, and Allen Bien-Aime were all charged by Complaint in the District of Rhode Island in connection with a scheme to obtain fraudulent UI and tax refund proceeds.[1] On October 13, 2020, the residences of Tony Mertile, Junior Mertile, James Legerme, as well as their persons and vehicles, were searched pursuant to federal search warrants. In addition to multiple computers and cell phones, law enforcement agents located:

a. At James Legerme residence, [redacted] NW 99th Terrace, Sunrise, FL (Legerme's residence) -- approximately $100,000 worth of jewelry and watches; $73,758 cash and money orders, multiple cellular

[1] The Complaints for Tony Mertile, Junior Mertile, James Legerme, and Allen Bien-Aime are docketed at Dkt Nos. 20-MJ-95, 20-MJ-96, 20-MJ-97, and 20-MJ-98. The cases were later charged by Indictment and Superseding Indictment, in the District of Rhode Island. *See* Dkt. No. 20-CR-00100.

telephones, and over one hundred debit cards in the names of other persons, including Chime debit cards and mailers.

b. At Tony Mertile's residence -- approximately $940,000 in cash, firearms, a large collection of jewelry and watches; a large number of debit cards in the name of other persons, from multiple banks, including Chime Bank, Wells Fargo bank, and SunTrust bank; multiple flip style cell phones marked with telephone numbers, including with Rhode Island area code (401); a notebook that appears to identify Green Dot and Go Bank accounts, among others.

c. At Junior Mertile's residence, -- $125,000 in cash, debit cards in the names of other persons, and multiple cell phones.

16. During a preview search of a cellular telephone located at (Legerme's residence, agents viewed text messages between the user of the telephone, believed to be Legerme and a contact identified as "Son" with telephone number +4[redacted]8084. The telephone number [redacted]8084 has been identified as one used by LUCKSON LOUISSAINT. The telephone number [redacted]8084 is the phone number listed in the subscriber information with Apple for an account in the name of "Luckson Louissaint" at "[redacted]coyle avenue, [redacted] pawtuket [sic], Rhode Island" with the Apple ID luck[redacted]@icloud.com. That phone number is also listed in the AirBNB user account for Luckson Louissaint. I also note that the contact information assigned to the number in cell phone located at Legerme's residence is "Son," which I believe to be an abbreviation for Luckson.

17. Based on the text messages exchanged between LOUISSAINT and Legerme, I believe that LOUISSAINT was provided Legerme, and his co-conspirators, with emails addresses and passwords to use in furtherance of the efforts to open fraudulent bank accounts and obtain fraudulent UI proceeds. Excerpts of some of the

messages are set forth below. In the messages, I have referred to the user of the cell phone as "Legerme" because the cell phone was found at his residence.

18. A text exchange dated March 28, 2020 reads:

-Legerme: 2:12 PM - You'll be done today?
-LOUISSAINT: 2:21 PM - Leb[redacted]@aol.com
Happyy05
60

Based on my training and experience, in this text message, I believe that LOUISSAINT was providing Legerme with an email address and password to access that email account.

19. A text exchange dated April 2, 2020 reads:

-Legerme: 2:59 PM - Still have 20 left but I'm giving it to t but I need lol (Emoji)
-LOUISSAINT: 2:59 PM - ok 100 more
-LOUISSAINT: 3:00 PM - ?
-Legerme: Yes go ahead, I owe you 200, P owe 100, Fat 100, T 100 right now.

Based on my training and experience, in this text message, I believe that Legerme was telling LOUISSAINT that he still had email addresses and passwords to be used, but that he was giving those email addresses/passwords to "t," who I believe to be co-conspirator Tony Mertile. I also believe that LOUISSAINT was confirming additional activity between them with his statement "ok 100 more." I also believe that Legerme was confirming what he and his co-conspirators owed LOUISSAINT, specifically that he (Legerme) owed LOUISSAINT $200 or owed for 200 email addresses and that his three co-conspirators, referenced by initials, owed him $100 each or for 100 email addresses. At this point, whether the numbers refer to amounts owed or email addresses created, for which money is owed, is not yet known. I also not that in text messages between Legerme and LOUISSAINT on March 22 and 23, 2020, there were references to "P/200, G/100/Fat/100. Text exchanged I owe you 200, P owe 100, Fat 100, T 100". I believe the references to "P," "Fat," "G," and "T," refer to Legerme's co-conspirators, including Junior Mertile, who is known by the name "Peanut," and Tony Mertile, who is referred to as "T."

20. A text exchange from April 4, 2020 reads:

-Legerme: I never paid you for Tony first 20
-LOUISSAINT: Emely [redacted]6@aol.com
Happy06

Based on my training and experience, in this text message, I believe that Legerme was telling LOUISSAINT that he owes LOUISSAINT money on behalf of co-conspirator TONY MERTILE for LOUISSAINT for LOUISSAINT's part in providing information, including e-mail addresses, to Legerme and others.

21. A text exchange from April 10, 2020 reads:

-Legerme: 10:06 AM - 12 didn't work
-LOUISSAINT: 10:08 AM - ok no problem
10:11 AM - asking for code?
-Legerme: 10:12 – yes

Based on my training and experience, in this text message, I believe that Legerme was telling LOUISSAINT that 12 of the email accounts and passwords that he provided didn't work and that when JAMES Legerme tried to access the accounts, he was prompted to enter a code.

18. A text message from June 6, 2020 reads:

-Legerme: 9:24 PM – Getting the money now for you

-LOUISSAINT: 10:38 PM – ok

Based on my training and experience, I believe that Legerme was advising LOUISSAINT that he was obtaining payment for him.

22. I have also reviewed bank records from Wells Fargo, that show that an account was opened in the name of Ryan P[redacted], DOB[redacted], listing LOUISSAINT's residence in Pawtucket, Rhode Island as the customer address. I have confirmed that Ryan P[redacted], with that DOB, is a real person and he does not reside in Pawtucket, Rhode Island. Based on my training and experience, I believe that a debit card for the Ryan P[redacted] account would have been sent to the address on file. From materials provided by Wells Fargo, this account and others, appear to be connected to

Tony Mertile, Legerme, and Junior Mertile. However, I note that the he investigation into the Wells Fargo activity is ongoing.

23. US Postal Service Records show that a priority mail parcel was sent, listing LOUISSAINT's home address and telephone number, [redacted]8084, to Legerme on August 25, 2020. A second parcel, a priority mail flat rate envelope, was sent from LOUISSAINT's address, the label image is partially cut off and no sender name can be seen, to Legerme on August 22, 2020. Based on my training and experience, and work on this investigation, I believe that LOUISSAINT was sending Legerme debit cards and/or PII for use in furtherance of the Specified Federal Offenses.

The October 13, 2020 Coyle Ave Search of LOUISSAINT's residence

24. On October 13, 2020, the Honorable Patricia A. Sullivan, US Magistrate Judge for the District of Rhode Island authorized search warrants for LOUISSAINT's residence [redacted] Coyle Ave [redacted] Pawtucket, RI, and his person of LOUISSAINT.[2] On October 13, 2020, the FBI executed the search of LOUISSAINT's residence. Agents were unable to execute the search of his person because LOUISSAINT was not home at the time of the search of his residence. A woman who identified herself as LOUISSAINT's girlfriend told agents that LOUISSAINT was working.

25. During the search of LOUISSAINT's residence, agents found 3 Chime debit cards with the debit card mailers, in the names of Stevan H[redacted], Shane H[redacted] and Shawn H[redacted] addressed to [redacted] Coyle Ave [redacted] Pawtucket, RI.

26. I know from my training and experience that Chime is a financial technology company that offers overs on-line and app-based banking services. Banking services for Chime accounts and debit cards are provided by Stride Bank and Bancorp Bank. Records produced by Stride Bank and Bancorp showed that each of these cards were issued in three different names, using SSNs and DOBs of three real persons, and

[2] Case Numbers: 20-SW-375-PAS and 20-SW-376-PAS

all were sent to LOUISSAINT's residence. We have not yet determined if these numbers and emails are legitimate with whom that are associated.

27. Stride Bank records showed that:

a. A person applied for the debit card in the name of Stevan H[redacted] on June 17, 2020 at 1:55 pm, using SSN [redacted] and DOB [redacted]. The listed account address was [redacted] Coyle Avenue, Pawtucket, RI 02860.[3] An $8,121.00 payment from Arizona Benefitpay, which services the Arizona UI agency, was made to this debit card on June 18, 2020. The AZ UI payment was for a claim filed on June 17, 2020 in the name of Shannon H[redacted], SSN [redacted], with a listed Arizona address. I have confirmed that a Shannon H[redacted], with this SSN, lives in Washington. The application information for each of the debit cards listed a phone number and email.

b. A person applied for the debit card in the name of Shane H[redacted] on June 17, 2020, at 1:47 pm (8 minutes before the Stevan H[redacted] application), using SSN [redacted] and DOB [redacted]. The records from Stride Bank show no deposits on the debit card in the name of Shane H[redacted].[4]

28. Bancorp records showed that a Chime debit card in the name of Shawn H[redacted] issued on June 17, 2020. The applicant listed the name Shawn H[redacted], and the SSN ending [redacted] and DOB of [redacted].[5] The records from Bancorp show no deposits on the debit card in the name of Shane H[redacted]. According to Bancorp records,

[3] The listed phone number on the Stevan H[redacted] Stride (Chime) account was [redacted]0737 and the email was mig[redacted]@aol.com.
[4] The listed phone number on the Stevan H[redacted] Stride (Chime) account was [redacted]5942 and the email was jua[redacted]@aol.com.
[5] The listed phone number on the Shawn H[redacted] Bancorp (Chime) account was [redacted]8157 and the email was rau[redacted]@aol.com.

the debit card in the name of Shane H was directed to be sent to "SHAWN H , COYLE AVE PAWTUCKET, RI 02860."

29. From my training and experience, and work on this investigation, I believe that the debit cards on which no deposits were made were opened to receive fraudulent UI benefits but we obtained the cards before they were used for that purpose.

Use of Real Identities

30. In addition to the use of the name Shannon H , as described above, in connection with the AZ UI claim, I have confirmed that the identifiers used to open the 3 Chime debit cards that were sent to LOUISSAINT's house all belong to real persons, whose DOBs and SSNs match the information use to open the accounts. None of the persons reside in LOUISSAINT's residence, the location listed as the address upon opening of the debit card accounts.

a. The true name, DOB, and SSN of Stevan H were used to open and the Stride Bank issued Chime card found at LOUISSAINT's residence and on which $8,121.00 in Arizona UI benefits were paid. Stevan H resides in Washington State.
b. The true name, DOB, and SSN of Shane H were used to open and the Stride Bank issued Chime card found at LOUISSAINT's residence and on which $8,121.00 in Arizona UI benefits were paid. Shane H resides in Oregon.
c. The true name and DOB of Shawn H were used to open the Bancorp issued Chime card found at LOUISSAINT's residence. Shawn H is a resident of Washington state, not of LOUISSAINT's residence in Pawtucket, Rhode Island.

Statement by LOUISSAINT

31. On October 21, 2020, LOUISSAINT called your affiant at the FBI Providence Office and asked to discuss the search warrant that had been executed at his

home on October 13, 2021. LOUISSAINT claimed that James Legerme was his cousin and that the package that LOUISSAINT sent to Legerme in Florida was a gift card. I note that the mail records obtained to date show that LOUISSAINT sent two, not one mailings, to Legerme, in August. LOUISSAINT spent $26.35 to send one parcel, and $7.75 to send the second parcel.

32. LOUISSAINT also claimed that he did make email addresses for Legerme, but it was for Legerme to use to give his business and AirBNBs good reviews. LOUISSAINT claimed he made 20 emails at one time and 20 or 30 email addresses another time. According to records from AirBNB, Legerme is not an AirBNB host. Legerme's wife, Shemka Williams is a host of one AirBNB property in Fort Lauderdale, FL. However, AirBNB records show that there are only 13 reviews for that property, and the last five reviews were March 1, March 11, March 15, March 21, and April 3, 2020. I note that LOUISSAINT's and Legerme's messages described above occurred between March 22, 2020 and June 6, 2020.

33. LOUISSAINT also acknowledge that he knew Tony Mertile. He claimed that both Legerme and Tony Mertile helped him when he first came to the country and was down on his luck. LOUISSAINT said that the last time he spoke to Tony Mertile was in 2017 when he called him to wish him a happy birthday.

34. Based on my training and experience in investigating this and similar violations of federal law, I believe that LOUISSAINT is a willing participant involved the UI fraud. I believe that LOUISSAINT assisted Legerme, Tony Mertile, Junior Mertile and others commit UI fraud by making email addresses for them. I believe that LOUISSAINT was paid for his services for making these emails and that is what is referenced in the text messages between Legerme and LOUISSAINT referenced in the October 2020 Riportella Affidavit. I believe that the Chime card located inside LOUISSAINT's apartment with the $8,121 of Arizona BenefitPay was payment for his services.

Additional UI Claims Associated with LOUISSAINT's Address

35. I am also aware that additional UI claims, in Rhode Island and in other states, list other persons and apartments in [redacted] Coyle Avenue, Pawtucket in UI applications. The IP addresses used to file those UI claims may be linked to additional UI claims for other addresses in multiple states. Our investigation is ongoing and we have not yet determined if those claims are valid and/or connected to LOUISSAINT.

Summary

36. Based on my training and experience, I believe that LUCKSON LOUISSAINT is conspiring with others, including James Legerme, Tony Mertile, Junior Mertile, and others, in the commission of the Specified Federal Offenses by providing information, including e-mail addresses and passwords, to his co-conspirators to open bank accounts and file fraudulent UI claims, and that he is knowingly receiving debit cards that were fraudulently issued in the names of others, to receive fraud proceeds.

37. The investigation into LOUISSAINT's conduct is ongoing. From a preliminary review of data from the Department of Labor, Office of the Inspector General, LOUISSAINT appears to be connected, through co-conspirators, to fraudulent UI claims in multiple states. However, the respective roles of LOUISSAINT and his co-conspirators, and the full scope of the conduct has not yet been determined.

38. Although an earlier search was conduct as LOUISSAINT's residence, I believe that additional evidence may be located at his residence. The nature of this fraud involved a complex scheme in which debit cards were issue in the names of others, and cards were mailed to persons, including LOUISSAINT, to facilitate the fraud. I believe that one or more banks, or UI agencies, may have sent materials to LOUISSAINT since the October 13, 2021 search. Further, as discussed above, we did not obtain LOUISSAINT's cell phone when the warrant was executed on October 13, 2021. As discussed above, the cell phone was used in the commission of the offense, and I believe that information relating to the Specified Federal Offenses will be located on LOUISSAINT's cell phone.

Evidence Obtained During Residential Searches

39. Based on my training and experience, I know that during the course of residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the SUBJECT PREMISES and computer devices located therein. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

40. Given the nature of this crime, I also believe it is reasonable to believe that the access devices, such as debit cards, and information relating thereto (names, social security numbers, passwords, online user log ins, etc.) would be maintained a place that allowed for safe storage, but ready access, such as a residence, for ATM or other debit transactions to be conducted shortly after the posting of fraudulent UI and/or tax refund payments to an account.

Evidence Relating to Fraud Offenses

41. Based on my training and experience and familiarity with investigations into fraud conducted by other law enforcement agents, I know the following:

a. Individuals maintain in their homes, both in paper and electronic format, among other items, records regarding the receipt and expenditure of money, documents relating to the purchase of assets, and records pertaining to their employment or business, even if that business is an illicit business.

b. Given the nature of fraud, I believe that participants in a long running fraud that involves several participants, more often than not, will keep records containing names, addresses, email addresses, and telephone numbers of co-conspirators, as well as targets and victims, amounts received from them, and amounts sent to co-conspirators. These records are necessary to further the

illicit fraud business and can be found in paper form or stored electronically in cell phones and other electronic devices. Owing to the long-term usefulness of such items, and tracking relative proceeds among co-conspirators, this type of evidence would likely be generated, maintained, and then possibly forgotten about and not disposed of.

c. I also know that those who make use of stolen personal identification as part of their fraud schemes, will often keep lists of the stolen PII, and notations on how and when that identify may be used, and any passwords for that "identity." I am also aware that fraudsters often maintain such documents related to their criminal activities at their residences or other locations over which they have control for an extended period of time, due to the high value associated with stolen PII that has been successfully used.

d. From training and experience, I know that individuals who amass proceeds from illegal activities routinely attempt to further that conduct and/or conceal the existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, credit and debit cards, money drafts, traveler's checks, wire transfers, etc. Records of such instruments, including ATM receipts, are oftentimes maintained at the individual's residence.

e. There are many reasons why criminal offenders maintain evidence for long periods of time. First, to the offender, the evidence may seem innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, checkbooks, videotapes and photographs,

utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered in light of other evidence. Second, the criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed computer-related evidence, which in fact, may be retrievable by a trained forensic computer expert. Thus, records and ledger-type evidence that one would think a prudent person might destroy because of its incriminatory nature are sometimes still possessed months or even years after the records were created.

f. Based on my knowledge with respect to facts and circumstances in this investigation, as well as my experience and training relating to cases involving individuals engaged in fraud schemes, as well as my discussions with other agents who investigated such cases, I know that it is a common practice for individuals engaged in these illegal activities to maintain the items and records or documents as set forth in Attachments B-1 through B-2, whether maintained on paper, in hand-written, typed, photocopied, or printed form, or electronically on a computer or cell phone, hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media, or any other storage medium.

Training and Experience on Digital Devices

42. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

43. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to,

one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

44. The search warrant also requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the user's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the user's face with her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

REQUEST FOR SEALING

45. Because this investigation is continuing and disclosure of some of the details of this affidavit may cause the targets or other affiliated persons to flee or further mask their identity or activities, destroy physical and/or electronic evidence, or otherwise obstruct and seriously jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

CONCLUSION

46. For all of the reasons described above, there is probable cause to arrest Luckson LOUISSAINT for the Specified Federal Offenses and to believe that the items to be seized described in Attachment B-1 and B-2, will be found in a search of the SUBJECT PERSON and SUBJECT PREMISES described in Attachment A-1 and A-2.

I declare that the foregoing is true and correct.

Matthew J. Riportella
Special Agent

FEDERAL BUREAU OF INVESTIGATION

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

_____	_____
Date	*Judge's signature*
Providence, RI	Lincoln D. Almond, US Magistrate Judge
City and State	*Printed name and title*